REMARKS

1. *Claim Amendments*

Applicants respectfully request entry of the foregoing amendments to claims 1, 7, and 20, and cancellation of claims 5, 6, and 24. Independent claims 1 and 20 have been amended as discussed further below. It is submitted that these amendments place the claims in condition for allowance; reconsideration and allowance of all claims is respectfully requested.

2. *Background*

Applicants first consider it useful to summarize the nature of the invention of amended claims 1 and 20, as well as the invention of U.S. Pat. No. 5,638,445 of Spelman et al. (below referred to as Spelman et al. '445).

A. *Amended Claims 1 and 20*

With reference to Fig. 1 of the present application, an embodiment according to the invention of amended claims 1 and 20 involves a communication module 107 (or corresponding method step) that establishes a communication connection between a sender, of one domain, and a receiver, in a different domain. For example, the sender may be a health services provider who possesses a large collection of medical data regarding its patients; and the receiver may be a medical researcher who wishes to examine statistical patterns in the medical data. In this case, the sender's domain is the domain of data collectors (such as the health services provider) and the receiver's domain is the domain of data analyzers (such as the medical researcher).

Coupled to the communication module 107, an embodiment according to the invention of claims 1 and 20 includes a mapping module 106 (or corresponding method step) which maps working data from one domain to the other. The working data includes an identifier portion and a research data portion. For example, the identifier portion may be a patient's name, in a medical record; and the research data portion may be the patient's medical data. In the invention of amended claim 1 (or corresponding method step of claim 20), the mapping module maps between the identifier portion of the data in one domain, into the identifier portion of the data in the other domain. For example, the mapping module 106 might encrypt the patient's name,

found in the data collector domain 109 of the health provider, so that the name becomes anonymous to the data analyzer 110.

Finally, an embodiment according to the invention of amended claims 1 and 20 includes a secret sharing module 108 (or corresponding method step) which controls access to the mapping module 106. In one example, the secret sharing module allows access to the mapping module only when a sufficient number of keyholders have provided passwords. For instance, as described at Specification pg. 10, lines 1-29 of the present application, the system may require N keyholders, prompting each for a password and certificate. The system may then concatenate all of the N passwords into a single combined password, and apply a predefined message-digest function onto the combined password to generate the encryption key, $K = MD (pw_1 + pw_2 + ... + pw_N)$, which is used to control access to the mapping. Because of this use of secret sharing, the key K that controls the mapping is unknown to any group of keyholders smaller than N.

An embodiment according to the invention of amended claims 1 and 20 therefore solves the problem of how to communicate data packets composed of personal identifiers and personal data between different domains, such that the personal identifiers are rendered anonymous by a mapping, access to which is controlled by secret sharing.

B. *Spelman et al. '445*

By contrast, Spelman et al. '445 relates to a method of processing encrypted communications sent by a consumer, typically to acquire goods from a merchant. There are generally four parties involved, as shown in Fig. 1: a consumer 10, who sends an order; a merchant 20, who receives the consumer's goods and services order (GSO); a merchant acquirer 40, such as a bank for the merchant, who processes the consumer's purchase instruction (PI) using the consumer's credit card number; and a recryptor 30, who acts as an encryption intermediary to ensure that only the proper parties have access to certain information in the transaction.

In particular, using various encryption and blinding functions, applied to data communicated between the parties, as summarized by the arrows in Figs. 1 and 2A-2D, the merchant ultimately obtains access to the consumer's goods and services order (GSO) using a

shared key k_1; and the merchant acquirer ultimately obtains access to the consumer's purchase instruction (PI) and credit card number using a shared key k_2.

In essence, Spelman et al. solves a key distribution problem, in which the merchant 20 is given access to shared key k_1; the merchant acquirer 40 is given access to shared key k_2; while the consumer does not know the public keys of either the merchant 20 or the merchant acquirer 40, but does know keys k_1 and k_2, and the public key R of the recryptor 30. The essence of Spelman et al.'s solution to this key distribution problem is summarized by the flow of data between the parties shown by the arrows in Figs. 1 and 2A-2D.

3. *Patentability of Claims as Amended*

With the foregoing as background, applicants respectfully traverse the rejection of claims 1-39 under 35 U.S.C. §103(a), and request reconsideration and allowance of those claims. The §103 rejections are in view of Spelman et al. '445 alone or in various combinations with Schneier, Ansell et al. and/or Coss et al. By comparing the claim language of independent claims 1 and 20, as now amended, with Spelman et al. '445, applicants respectfully submit that the invention of those claims is neither disclosed nor suggested by Spelman et al. '445.

In particular, the language of amended claim 1 includes "a secret sharing module for controlling access to the mapping module"; a corresponding method step is included in amended claim 20. As described above, such a secret sharing module may (in one example) allow access to the mapping module only when a sufficient number of keyholders have provided passwords. Controlling access to the mapping using secret sharing provides several advantages, including that, as stated at Specification pg. 10, lines 4-5, no single individual can compromise the secret mapping.

By contrast, Spelman et al. '445 neither discloses nor suggests the use of a secret sharing module to control access to a mapping module that maps identifiers from one domain to another. As described above, Spelman et al. '445 does involve encrypted communications between four parties, i.e. the consumer 10, the merchant 20, the merchant acquirer 40, and the recryptor 30.

Spelman et al. '445 does not, however, disclose or suggest the use of secret sharing to control access to any mapping that is used between any of the parties 10, 20, 30, 40.

Applicants respectfully traverse the statement in the Office Action with regard to former claims 5 and 6, that Spelman et al. '445 discloses a secret sharing module that controls access to a mapping module. The cited item at Fig. 1, part 30, is in fact the recryptor 30, who is one of the parties to the transaction. There is no disclosure or suggestion that the recryptor 30 requires entry of multiple keyholder passwords, or uses another secret sharing technique, in its operation.

With regard to the cited passage at Col. 6, lines 14-59 of Spelman et al. '445, this passage actually describes the merchant 20's use of a blinding function B to transmit data in Fig. 2B. This blinding function is used so that the recryptor 30 does not know the consumer's credit card number. However, Spelman et al. '445 does not disclose or suggest that the merchant 20 requires entry of multiple keyholder passwords, or uses another secret sharing technique, in this transmission.

Accordingly, applicants respectfully submit that Spelman et al. '445 neither discloses nor suggests the use of a secret sharing module to control access to a mapping module. It is therefore submitted that independent claims 1 and 20, as now amended are not obvious over the cited art; and therefore these claims, and their dependent claims, are allowable.

In addition, Applicants also submit that claims 1 and 20 are not obvious over Spelman et al. '445 because the Recryptor service of Spelman et al. '445 does not handle data that can be split into an identifier portion and a research portion. The Recryptor of Spelman et al. '445 obtains the merchant name and, based on it and the merchant acquirer, recrypts

the two data packets, one for the merchant and one for the merchant-acquirer. Thus the Recryptor uses the names (the identifiers) to select from the directory the appropriate public-keys, which it then uses to encrypt the two packets with k1 and k2. By contrast, in an embodiment according to claims 1 and 20, only the identifier portion is encrypted (mapped between domains). In Spelman et.al., the merchant name, and the merchant-acquirer which by definition is in a different domain than the merchant, are more like target domains; and the Recryptor selects a mapping module (public-key) based on the target. However, the Recryptor service encrypts all of the data; whereas in an embodiment according to claims 1 and 20, only the identifier portion is encrypted/mapped. Therefore, for this reason in addition to those given above, applicants submit that claims 1 and 20 are not obvious over Spelman et al. '445.

Dependent claims 3-4, 9-12, 22-23 and 27-30 were rejected under 35 U.S.C. §103 over Spelman et al. '445 combined with Schneier. By virtue of their dependency on base claims 1 and 20, the foregoing arguments for claims 1 and 20 apply here. Further, Schneier does not add to Spelman et al. '445 the use of secret sharing to control access to a subject mapping. Without such secret sharing, no combination of Schneier and Spelman et al. '445 makes obvious the present invention as now claimed. Withdrawal of this §103 rejection of claims 3-4, 9-12, 22-23 and 27-30 is respectfully requested.

Dependent claims 13-15, 31-33 and 38 were rejected under 35 U.S.C. §103 based on Spelman et al. '445 in view of Ansell et al. These claims depend from respective base claims 1 and 20, and thus the foregoing arguments apply. Ansell et al. does not add to Spelman et al. '445 the use of secret sharing to control access to the subject mapping as in the invention as now claimed. As such, no combination of Ansell et al. and Spelman et al. '445 makes obvious the present invention of claims 13-15, 31-33 and 38. This rejection is therefore believed to be overcome.

Claim 39 has been rejected under 35 U.S.C. §103 based on Spelman et al. '445 in view of Coss et al. Claim 39 depends from claim 1 and thus inherits the patentable distinctions (and claim limitations) discussed above. Coss et al. does not add the present invention's secret sharing control of access to a mapping, which is missing from Spelman et al. '445. As such, no combination of Spelman et al. '445 and Coss et al. can make the present invention obvious. Withdrawal of this rejection is respectfully requested.

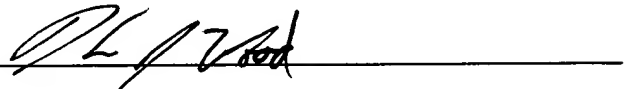
CONCLUSION

In view of the above amendments and remarks, it is believed that all claims as now amended (claims 1-4, 7-23 and 25-39) are in condition for allowance, and it is respectfully

requested that the application be passed to issue. If the Examiner feels that a telephone conference would expedite prosecution of this case, the Examiner is invited to call the undersigned.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By 

Keith J. Wood
Registration No. 45,235
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133
Dated: December 8, 2004